UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,667	09/30/2003	Germano Caronni	03226/296001; P9007	5817

32615 7590 04/03/2009

OSHA LIANG L.L.P./SUN
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	**PAPER NUMBER**
2439	

NOTIFICATION DATE	DELIVERY MODE
04/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
lord@oshaliang.com
hathaway@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/675,667	CARONNI, GERMANO	
	Examiner	Art Unit	
	Farid Homayounmehr	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☒ Claim(s) *15* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *30 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/9/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-30 have been examined.

Information Disclosure Statement PTO-1449

1. The Information Disclosure Statement submitted by the applicant on 1/9/2004 has been considered. Please see attached PTO-1449.

Claim Objections

2. Claim 15 is objected to because of the following informalities: The claim is dependent on itself. Examiner assumes that the claim is meant to be dependent on claim 14. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8-12, and 24-29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims are directed to layer-encrypted data blocks, however, the characteristics and attributes of layer-encrypted data blocks are not determined, and therefore it is

unknown how they further limit the claim. In describing layer-encrypted data blocks, applicant's Specification is directed to figure 7 and states: "*As illustrated in Figure 7, an encrypted data block or group of encrypted data blocks encrypted with a layer key is a layer-encrypted data block. For example, layer-encrypted data blocks A-C (500-504) are encrypted with layer key (524) and layer-encrypted data blocks D-G (506-512) are encrypted with layer key (522).*" However, the Specification has no definition or description of a layer key, and therefore, the characteristics and features associated with a layer–encrypted data block, and how it is distinguished from an ordinary encrypted data block are not clear.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 3, 4, 13, 14, 15, 20, 22, 23, and 30 rejected under 35 U.S.C. 103(a) as being unpatentable over Rothrock (US 7,149,900) hereinafter called Rot in view of Scheidt (US Patent No. 6,490,680).

5.1. As per claims 1, Rot is directed to a method for re-encrypting encrypted data in a secure storage file system , comprising:

obtaining selected data to re-encrypt from the secure storage file system using a

user data access record and the encrypted data (Rot col. 4 lines 57-65 teaches a system for accessing an encrypted secure storage module. The system uses an agent's API to obtain properly authorized access (col. 5 lines 29-32), and allows updating and re-encrypting the data in the secured memory. To determine proper authorized access, Rot must use user data access record);

decrypting the selected data using a symmetric key (Rot teaches access to encrypted data, decrypting and re-encrypting data, but does not explicitly detail the type of keys, and data elements involved in encryption, decryption and re-encryption.

Scheidt is directed to a system for controlling access to data. Scheidt uses keys to control access to information based on the role of users (col. 4 lines 15-31). Scheidt figures 1 and 2 describe the process of data encryption and decryption. Figure 2 and associated text describes the decryption of data which was encrypted in the system. Col. 17 lines 15-35 shows how encrypted data is decrypted. As shown in col. 3 lines 64-67, Scheidt teaches that both symmetric and asymmetric keys can be used for encryption and decryption);

re-encrypting the selected data using a new symmetric key to obtain new encrypted data (Scheidt Fig. 1 and associated text, particularly, col. 16 lines 49-50, and 60-62, where it shows that the data is encrypted using the working split key. Note again that as mentioned above, Scheidt teaches use of symmetric and asymmetric keys for encryption and decryption. Also note that Rot teaches the need for re-encrypting data, and Scheidt teaches the associated details);

encrypting the new symmetric key using a public key to obtain a new encrypted symmetric key (Scheidt Fig.1 and 2 and associated text, where the key used to encrypt the data (working split) is encrypted. Note that as shown in Fig. 2, the encrypted data is decrypted using the same working split that was used to encrypt the data (col. 17, lines 30-36). Furthermore, the working split was never stored in plain text. The elements of working split were encrypted (col. 16, lines 50-65) and then decrypted to reconstruct the working split. Therefore, the working split was encrypted and then decrypted. In addition, Scheidt teaching of encrypting the elements of a key makes encrypting the key obvious);

storing the new encrypted data and the new encrypted symmetric key if the public key is associated with a file system user having read permission (Scheidt teaches that the user who has read permission is provided with data elements necessary to perform data decryption: Scheidt col. 16 line 62 to col. 17 line 11 shows information needed to decrypt the data is constructed and stored in the workstation and user Super Card. This information includes the working split, and the encrypted data. Column 16 lines 11-18 shows that Key splits and labels are used to determine who can encrypt and decrypt data. Column 10 lines 60-64 shows that the user who has labels necessary to decrypt, has read permission. Therefore the user with read permission is provided with keys and labels to decrypt (see col. 16 lines 31-33). As mentioned above, the information needed to decrypt is provided to the user, and includes the working split and the encrypted data. Therefore, the working split and encrypted data is stored when user has read permission.

Scheidt also teaches that determining if the user has read permission is made based on user credentials: The public key is a credential of the user, and Scheidt teaches using the user credentials in generation and construction of the split keys as explained above and noted in col. 16 lines 10-19);

storing an encrypted hash data if the file system User has write permission (Fig. 1 shows that the plaintext data is hashed and encrypted. Similar to the read permission, the user must have write permission to encrypt (col. 16 lines 20-25, and col. 10 lines 60-64), and Scheidt provides the elements necessary to perform encryption to the user authorized to perform encryption (has write permission)).

Scheidt and Rot are analogous art as they are both directed to a secure data access control system. At the time of invention, it would have been obvious to the one skilled in art to improve Rot's system of secure data access control during the time when data is updated, by including the keys and labels of Scheidt to further secure the system by limiting access to users with proper permission (Scheidt col. 4 lines 15-30).

5.2. Limitations of claim 20 are substantially the same as claim 1, with the added limitation of a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the encrypted data. Rot in view of Scheidt teaches the added limitation: As shown in claim 1, a re-encryption event will be followed by generation and re-encryption of keys, and therefore, it generates a key re-encryption event. Scheidt col. 2 lines 4-58 shows that a user

device (client) can connect the server and access the server, which involves initiation of the method of claim 1. Therefore, Scheidt's user device (client) generates a key re-encryption event. Note also that Scheidt's user device includes an application which uses the encrypted data, and includes a kernel.

5.3. Limitations of claims 13 and 30 are substantially the same as claim 1, and directed to the hardware and apparatus performing the operations and steps of claim 1. Rot in view of Scheidt also teaches hardware and apparatus necessary to perform operations and steps.

5.4. As per claims 3 and 4, Rot in view of Scheidt is directed to the method of claim 1, wherein the write permission comprises at least one sub-division and the sub-division is selected from a group consisting of insert, append, truncate, and delete (Scheidt allows modification of data when the user has write permission. The "write" operation is regarded as any general operation that involves data modification, which includes insert, append, truncate, and delete.)

5.5. Limitations of claims 14, 15, 22 and 23 are substantially the same as claims 3 and 4. Also see rejection of claims 13 and 30.

6. Claims 2, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothrock (US 7,149,900) hereinafter called Rot in view of Scheidt (US Patent No. 6,490,680), and further in view of Zheng (US Patent No. 6,556,994).

6.1. As per claim 2, Rot in view of Scheidt is directed to the method of claim 1. Rot in view of Scheidt teaches accessing data based on user access data record (credentials). However, Rot in view of Scheidt does not explicitly teach using a bit map as user access data record.

Zheng teaches using bitmap as user access data record (Fig. 2 and associated text). At the time of invention, it would have been obvious to use the bitmap of Zheng in developing user access data record. The motivation would be to use a well-practiced and easy to develop method of implementing access data record such as bitmaps.

6.2. Limitations of claims 19 and 21 are substantially the same as claim 2. Also see rejection of claims 13 and 30.

7. Claims 5-7, 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothrock (US 7,149,900) hereinafter called Rot in view of Scheidt (US Patent No. 6,490,680), and further in view of Quarato (US Patent No. 6,253,205).

7.1. As per claims 5, 6 and 7, Rot in view of Scheidt is directed to the method of claim 1, however, it does not explicitly teach wherein the secure storage file system is implemented using a preloaded shared library, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses, and the shared library includes functionality to map read/write/file name accesses to a custom-implemented file system. Quarto is directed to a translation framework, which performs data conversions (see abstract). Quarato col. 3 line 65 to col. 4 line 40 teaches a translator using shared libraries that can convert data objects (such as read/write/file name accesses), and map the data objects to work in a different platform (col. 4 lines 25-30). At the time of invention, it would have been obvious to implement the system of Rot in view of Scheidt using the shared libraries as taught by Quarato. The motivation would be to include the benefits of the object oriented programming in the implementation of the system, as noted by Quarato col. 2 lines 17-40.

7.2. Limitations of claims 16, 17 and 18 are substantially the same as claims 5, 6, and 7. Also see rejection of claim 13.

8. Claims 8, 10-12, 24, and 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothrock (US 7,149,900) hereinafter called Rot in view of Scheidt (US Patent No. 6,490,680), and further in view of Saito (US Patent No. 7,324,644).

8.1. As per claims 8, 10 and 11, the requirements of claims 8, 10 and 11 are substantially the same as claim 1, and made obvious by Rot in view of Scheidt as discussed above, expect that claim 8 requires re–encrypting layer-encrypted data blocks. As defined by applicant, layer-encrypted data blocks are data blocks encrypted by a layer key. Saito is directed to encrypting data using a layer key at col. 10, lines 10-18. At the time of invention, it would have been obvious to use the layer key as shown by Saito to perform the data encryption in the system of Rot in view of Scheidt. This is because using a layer key is just a design choice without limiting or disrupting the system, and it allows the system to work with Bluetooth compatible systems, as indicated by Saito.

8.2. Limitations of claims 24, 26, 27 and 29 are substantially the same as claims 8, 10, and 11. Note that claim 24 has the added limitation of a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the encrypted data. Rot in view of Scheidt teaches the added limitation: As shown in claim 1, a re-encryption event will be followed by generation and re-encryption of keys, and therefore, it generates a key re-encryption event. Scheidt col. 2 lines 4-58 shows that a user device (client) can connect the server and access the server, which involves initiation of the method of claim 1. Therefore, Scheidt's user device (client) generates a key re-encryption event. Note also that Scheidt's user device includes an application which uses the encrypted data, and includes a kernel.

8.3. As per claim 12, Scheidt col. 11 lines 15-20 teaches an authentication agent which provides the credentials (the layer key and new layer key).

8.4. Limitations of claim 28 are substantially the same as claim 12. Also see rejection of claim 13.

9. Claims 9 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothrock (US 7,149,900) hereinafter called Rot in view of Scheidt (US Patent No. 6,490,680), and further in view of Saito (US Patent No. 7,324,644), and further in view of Zheng (US Patent No. 6,556,994).

9.1. As per claim 9, Rot in view of Scheidt and Saito is directed to the method of claim 8. Rot in view of Scheidt and Saito teaches accessing data based on user access data record (credentials). However, Rot in view of Scheidt and Saito does not explicitly teach using a bit map as user access data record.

Zheng teaches using bitmap as user access data record (Fig. 2 and associated text). At the time of invention, it would have been obvious to use the bitmap of Zheng in developing user access data record. The motivation would be to use a well-practiced and easy to develop method of implementing access data record such as bitmaps.

9.2. Limitations of claim 25 are substantially the same as claim 9. Also see rejection of claim 13.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Farid Homayounmehr/

Examiner

Art Unit: 2439